

FIG. 1

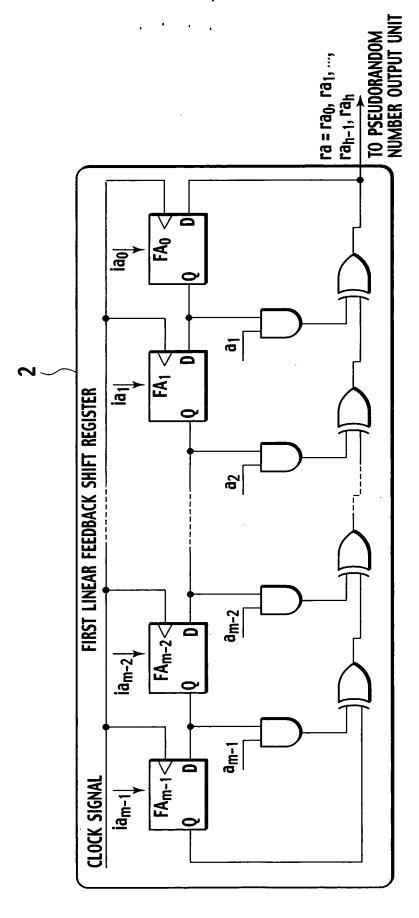


FIG. 2

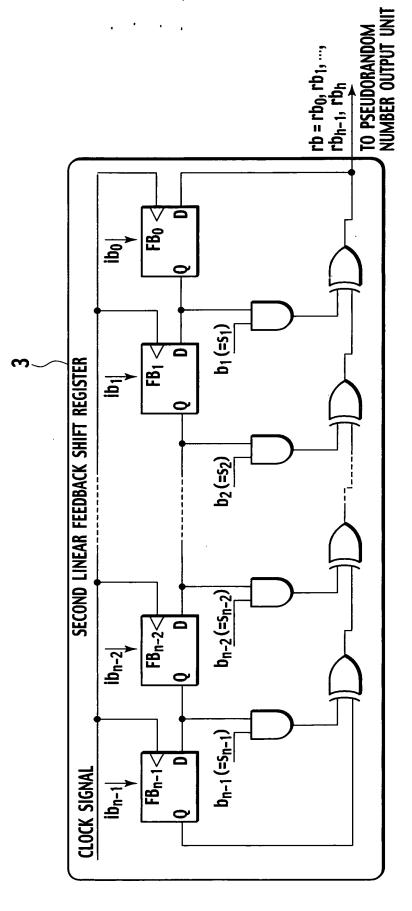


FIG. 3

FIG. 4

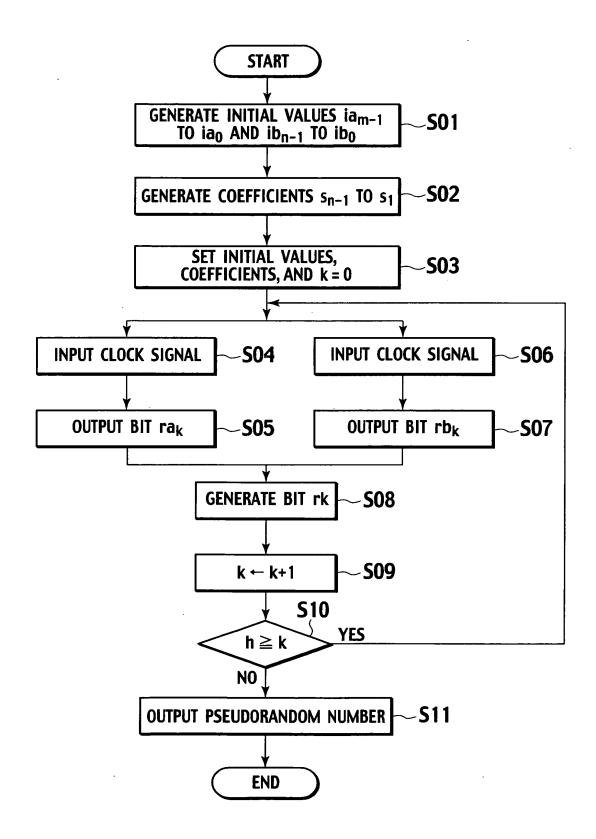


FIG. 5

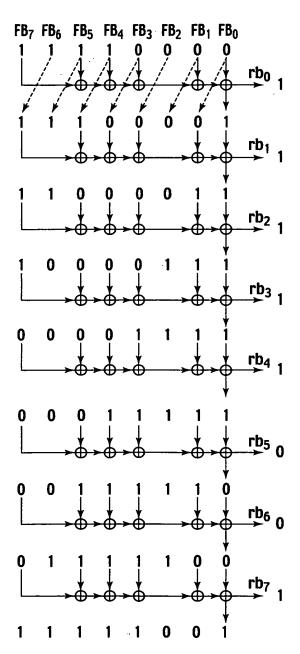
FIRST LINEAR FEEDBACK SHIFT REGISTER

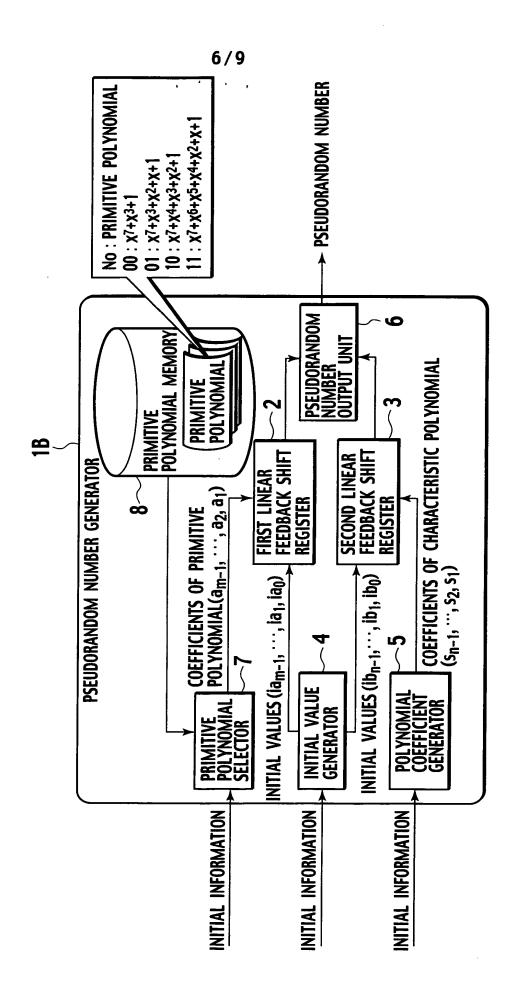
 $x^7 + x^3 + 1$ (a₆, a₅, a₄, a₃, a₂, a₁ = (000100)

INITIAL FA6 FA5 FA4 FA3 FA2 FA1 FA0 STATE ra₀0 +1 ra₁ 0 +2 0 0 0 1 ra₂0 +3 0 0 ra₃0 +4 0 0 0 1 0 ra₄ 1 +5 0 ra₅₀ +6 0 0 0 0 1 ra₆1 +7 0 0 0 0 ra₇ 1 0 0 0 1 1

SECOND LINEAR FEEDBACK SHIFT REGISTER

 $x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$





7/9 . FIG. 7 **START SELECT PRIMITIVE POLYNOMIAL -S21** GENERATE INITIAL VALUES ia_{m-1} TO ia₀ AND ib_{n-1} TO ib₀ **S22** GENERATE COEFFICIENTS s_{n-1} TO s_1 **-S23** SET INITIAL VALUES, COEFFICIENTS, AND k = 0 **S24** INPUT CLOCK SIGNAL INPUT CLOCK SIGNAL **S27 -S25 S26 S28 OUTPUT BIT rak** OUTPUT BIT rbk GENERATE BIT rk **-S29 S30** k ← k+1 **S31** YES $h \ge k$ NO **-S32 OUTPUT PSEUDORANDOM NUMBER END**

